(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23315 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/26495

(22) International Filing Date: 24 August 2001 (24.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/659,902 12 September 2000 (12.09.2000) US

(71) Applicant: PREVIEW SYSTEMS, INC. [US/US]; 1195 W. Fremont Avenue, Suite 2001, Sunnyvale, CA 94087 (US).

(72) Inventors: XU, Bin; 955 La Mesa Terrace, Unit-I, Sunnyvale, CA 94086 (US). LI, Weijun; 687 Ontario Court, # 8, Sunnyvale, CA 94087 (US). SMITH, Kyle; 394 Vale Drive, San Jose, CA 95123 (US). BAO, Dalun; 200 E. Dana St. D85, Mountain View, CA 94041 (US).

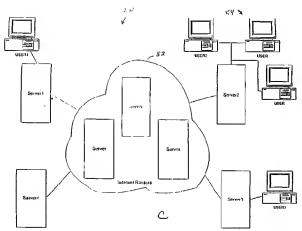
(74) Agents: NWAMU, Fidel, D. et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111 (US).

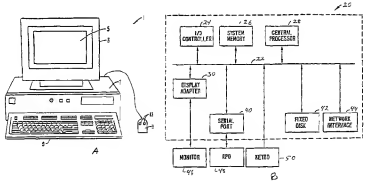
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT





(57) Abstract: A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.

WO 02/23315 A2

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT

BACKGROUND OF THE INVENTION

This invention relates to the field of information processing and more particularly to systems for implementing digital management rights.

Millions of users currently have access to more information than at any period in the history of society. Specifically, digital content such as interactive web content, musical recordings, medical and financial forms, automatic banking, facsimiles, and various other forms of audio and video content are widely accessible.

Although attributable to a number of reasons, the widespread access to digital content has been a result of the development of electronic compuer networks, and Internet in particular. Another reason relates to the increase in available bandwidth and the availability of compression technology for transferring large amounts of content. In addition, numerous sites and bulletin boards post content for distribution to users. Content providers such as publishers of books and magazines, information database providers, and producers of music, video games, and images are distributing content in digital form over the Internet. In fact, some providers of interactive web content and music provide interactive web players for playing back content. Examples of such interactive web players which are currently available on the market are Quicktime 4™ available from Apple Computer, Inc.®, RealPlayer™ available from RealNetworks, Inc. ® and Shockwave 7™ available from MacroMedia, Inc. ®

While access to digital content has been widely beneficial, a fundamental problem facing content providers is how to prevent the unauthorized use and distribution of digital content. Content providers are concerned with getting compensated for their work. Unauthorized copying and use of content providers works deprives rightful owners of billions of dollars according to a well-known source. Unauthorized copying is exercebated because consumers can easily retrieve content, and technology is available for perfectly reproducing content.

A number of mechanisms have been developed to protect against unauthorized access and duplication and to provide digital rights management. One method is a digital rights management system that allows a set of rules to determine how the content is used. Another method (for software) for curbing unauthorized duplication

is the use of a scheme which provides software tryouts or demos that typically work and expire after a specific duration. Other methods use a copy protection scheme that limits the number of copies that a user can make, after which additional copying results in corrupt copies. Further, an alternate scheme requires the presence of a license on a client workstation for the software to operate.

Many of the aforementioned schemes are typically implemented using "encryption/decryption" of the digital content. Encryption is the conversion of data into an unintelligible form, e.g., ciphertext, that cannot be easily understood by unauthorized users. Decryption is the process of converting encrypted content back into its original form such that the it becomes intelligible. Simple ciphers include the rotation of letters in the alphabet, the substitution of letters for numbers, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital information content.

In order to easily recover the encrypted information content, the correct decryption key is required. The key is an algorithm that decodes the work of the encryption algorithm. The more complex the encryption algorithm, the more difficult it becomes to decode the communications without access to the key. Generally, there are two types of key schemes for encryption/decryption systems, namely (1) Public Key Systems (PKS) or asymmetric systems which utilize two different keys, one for encryption, or signing, and one for decryption, or verifying; and (2) nonpublic key systems that are known as symmetric, or secret key, systems.

Although the use of public or private key can be an effective way to prevent access to digital content, the transfer of keys often requires extensive coordination with the end user. Also, the use of keys in the related art does not always provide flexible licensing arrangements, or an efficient way to handle many instances of different deliverable digital content products.

Therefore, there is a need to resolve the aforementioned problem relating to conventional approaches for protecting digital information particularly with regard to managing the digital rights for on-line distribution of interactive web content and music.

SUMMARY OF THE INVENTION

A system for managing rights to a content file within a computer network. The system permits streaming and allows an authorized user to play back the content file

while the user is online. In one embodiment, the system comprises a key for decrypting the content file, a license which contains the key for authorizing decryption and playback of the content file and a header which contains information relating to a name for the license, identification of the content file, and a URL (uniform resource locator) of the server. Advantageously, a content module encrypts the content file, removes a portion of the content file and substitutes the header thereof.

Upon request, a user's computer system receives the content file and the license via a communication network. When the content file and the license have been received, a decoder module decrypts the content file using the key, which is contained within the license. In a further aspect, a license data generator generates a machine identification to which the license is bound so that the content file is playable only on the designated machine. The system further includes a core module for retrieving the identification information from the license data generator, a license database for storing the license when received, and a content player which plays back the content file when it is unencrypted. In this manner, the present invention permits both playback of the content file and management of the corresponding rights to the content file without the disadvantages associated with the related art.

In one embodiment, the present invention provides a system for encrypting a content file within a computer network for on-line playback. The system comprises a first key for decrypting the content file and a header which contains information that allows playback of the content file. Other components include a key module for generating the first key, and a content module for encrypting the content file, and for removing a first content portion of the content file and substituting the header thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is an illustration of computer system 1 including display 3 having display screen 5.

Fig. 1B illustrates subsystems that might typically be found in a computer such as computer 1.

Fig. 1C is a generalized diagram of a typical network.

Fig. 2 is a block diagram of a zipLock system for encrypting content files according to the present invention.

Fig. 3 is a schematic block diagram of a zipLock delivery system for delivering encrypted content to an end user disk.

Fig. 4 is a schematic block diagram of a zipLock system for enabling playback of content files according to the present invention.

Fig. 5 is a block diagram of a zipLock system for acquiring a license which authorizes a user to playback a content file.

DETAILED DESCRIPTION OF THE DIAGRAMS

Overview

A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.

Therefore, at the very least, one or more keys and a license are required in order for a user to play back a content file. In this manner, the present system manages digital rights pertaining to such content files in accordance with one embodiment of the present invention. The present invention will be further understood with reference to the diagrams and descriptions which follow.

Description of Hardware

Fig. 1A is an illustration of computer system 1 including display 3 having display screen 5. Cabinet 7 houses standard computer components (not shown) such as a disk drive, CDROM drive, display adapter, network card, random access memory (RAM), central processing unit (CPU), and other components, subsystems and devices. User input devices such as mouse 11 having buttons 13, and keyboard 9 are shown. Other user input devices such as a trackball, touch-screen, digitizing tablet, etc. can be used. In general, the computer system is illustrative of but one type of computer system, such as a desktop computer, suitable for use with the present invention. Computers can be

configured with many different hardware components and can be made in many dimensions and styles (e.g., laptop, palmtop, pen top, server, workstation, mainframe). Any hardware platform suitable for performing the processing described herein is suitable for use with the present invention.

Fig. 1B illustrates subsystems that might typically be found in a computer such as computer 1.

In Fig. 1B, subsystems within box 20 are directly interfaced to internal bus 22. Such subsystems typically are contained within the computer system such as within cabinet 7 of Fig. 1A. Subsystems include input/output (I/O) controller 24, System Random Access Memory (RAM) 26, Central Processing Unit (CPU) 28, Display Adapter 30, Serial Port 40, Fixed Disk 42 and Network Interface Adapter 44. The use of bus 22 allows each of the subsystems to transfer data among the subsystems and, most importantly, with the CPU. External devices can communicate with the CPU or other subsystems via bus 22 by interfacing with a subsystem on the bus. Monitor 46 connects to the bus through Display Adapter 30. A relative pointing device (RPD) 48 such as a mouse connects through Serial Port 40. Some devices such as Keyboard 50 can communicate with the CPU by direct means without using the main data bus as, for example, via an interrupt controller and associated registers (not shown).

As with the external physical configuration shown in Fig. 1A, many subsystem configurations are possible. Fig. 1B is illustrative of but one suitable configuration. Subsystems, components or devices other than those shown in Fig. 1B can be added. A suitable computer system can be achieved without using all of the subsystems shown in Fig. 1. For example, a standalone computer need not be coupled to a network so Network Interface 44 would not be required. Other subsystems such as a CDROM drive, graphics accelerator, etc. can be included in the configuration without affecting the performance of the system of the present invention.

Fig. 1C is a generalized diagram of a typical network.

In Fig. 1C, the network system 80 includes several local networks coupled to the Internet. Although specific network protocols, physical layers, topologies, and other network properties are presented herein, the present invention is suitable for use with any network.

In Fig. 1C, computer USER1 is connected to Server1. This connection can be by a network such as Ethernet, Asynchronous Transfer Mode, IEEE standard 1553 bus, modem connection, Universal Serial Bus, etc. The communication link need not be a

wire but can be infrared, radio wave transmission, etc. Server1 is coupled to the Internet. The Internet is shown symbolically as a collection of server routers 82. Note that the use of the Internet for distribution or communication of information is not strictly necessary to practice the present invention but is merely used to illustrate a preferred embodiment, below. Further, the use of server computers and the designation of server and client machines is not crucial to an implementation of the present invention. USER1 Computer can be connected directly to the Internet. Server1's connection to the Internet is typically by a relatively high bandwidth transmission medium such as a T1 or T3 line.

Similarly, other computers at 84 are shown utilizing a local network at a different location from USER1 computer. The computers at 84 are coupled to the Internet via Server2. USER3 and Server3 represent yet a third installation.

Note that the concepts of "client" and "server," as used in this application and the industry, are very loosely defined and, in fact, are not fixed with respect to machines or software processes executing on the machines. Typically, a server is a machine or process that is providing information to another machine or process, i.e., the "client," that requests the information. In this respect, a computer or process can be acting as a client at one point in time (because it is requesting information) and can be acting as a server at another point in time (because it is providing information). Some computers are consistently referred to as "servers" because they usually act as a repository for a large amount of information that is often requested. For example, a World Wide Web (WWW, or simply, "Web") site is often hosted by a server computer with a large storage capacity, high-speed processor and Internet link having the ability to handle many high-bandwidth communication lines.

A server machine will most likely not be manually operated by a human user on a continual basis, but, instead, has software for constantly, and automatically, responding to information requests. On the other hand, some machines, such as desktop computers, are typically thought of as client machines because they are primarily used to obtain information from the Internet for a user operating the machine.

Depending on the specific software executing at any point in time on these machines, the machine may actually be performing the role of a client or server, as the need may be. For example, a user's desktop computer can provide information to another desktop computer. Or a server may directly communicate with another server computer. Sometimes this is characterized as "peer-to-peer," communication. Although processes of the present invention, and the hardware executing the processes, may be characterized

by language common to a discussion of the Internet (e.g., "client," "server," "peer") it should be apparent that software of the present invention can execute on any type of suitable hardware including networks other than the Internet.

Although software of the present invention, may be presented as a single entity, such software is readily able to be executed on multiple machines. That is, there may be multiple instances of a given software program, a single program may be executing on two or more processors in a distributed processing environment, parts of a single program may be executing on different physical machines, etc. Further, two different programs, such as a client and server program, can be executing in a single machine, or in different machines. A single program can be operating as a client for one information transaction and as a server for a different information transaction.

Details of Embodiments of the Present Invention

A first embodiment of the present invention is incorporated into a product called "zipLock"™ available from a primary company Preview Systems, Inc.® of Sunnyvale, California.

Fig. 2 is a block diagram of zipLock system 200 for encrypting content files according to the present invention. As used herein, the term "content" refers to digital information.

In Fig. 2, among other components, system 200 comprises content builder module 216 for encrypting one or more digital files, DRM encoder 210 for coordinating encryption as well as providing a header, DRM key module 212 for associating the information contained within a content file with a license, and zipLock database 202 for storing key sheaves received from content builder 212.

In a typical content encryption procedure, content builder 216 receives a single unencrypted content file 206 (or multiple unencrypted content files 208) for encryption. Content files 206 may be a musical recording, an audio or video image, which may be from third party sources or directly from the content providers. Upon receiving content file 206, content builder 216 utilizes an encryption algorithm to implement the encryption process. In one embodiment, this process is accomplished by segmenting content file 206 into variable segments, each segment being encrypted with a separate key.

A "key" may be a variable value that is applied to content file 206 using an algorithm to produce encryption text. A single key or multiple keys having constant or

variable lengths may be employed depending on which embodiment is implemented. After the encryption process, the keys are saved in zipLock database 202 for later retrieval during the playback process. In an exemplary embodiment, database 202 is an industry standard database system such as Oracle 8™ available from Oracle, Inc.®

Content builder 216 also functions to interact with database 202 to create the necessary information to enable the sale, distribution and tracking of the content within system 200. Advantageously, during the encryption process, content builder 216 removes a portion of content file 206 and in its place inserts a header (not shown), supplied by DRM encoder 210. The removed portion is thereafter added to a license file for authorizing playback of the content file 206. Therefore, the removed portion is considered part of the keys. Depending on the embodiment being implemented, the removed portion may be added to a pre-configured license, the terms of which are predefined. During the playback process, the pre-configured license is then retrieved when its terms are the same as the user's transaction. Alternatively, the removed portion may be saved and later added to a license which is generated on the fly during the playback process. In any event, once the license is obtained, the removed portion is thereafter recombined with the original content portion during the playback process.

Advantageously, removing a portion of content file 206 also provides a measure of extra security as the removed portion of content file 206 remains unavailable until decryption time. Therefore, copying encrypted content to another machine is completely useless without the back binding license. A further reason for removing a portion of content file 206 to accommodate the header is to keep the content file the same length as the original file. In this manner, the process of seeking a specific location in content file 206 during the decryption process is simplified.

The header within content file 206 contains information fields such as the license name, the content file identification, and the license server URL (uniform resource locator). The license name field enables content file 206 to be associated with the license file (containing the removed content portion). The content identification field identifies the content file 206 while the license server URL points to the address of the license server where the license is generated (or located). Although a multiple-field header is not shown, one of ordinary skill in the art will realize that the header may contain multiple fields for identifying various types of information other than those referenced above.

Fig. 3 is a schematic block diagram of zipLock delivery system 300 for delivering encrypted content 304 to an end user disk 310.

In Fig. 3, delivery system 300 includes content server 302 for generating encrypted content 304, interactive web player 312 and DRM proxy 308 which provides an alternate means for retrieving encrypted content 304 from server 302. Although operable in a number of modes, in one embodiment, system 300 functions in an on-line mode. In this mode, content 304 remains on content server 302 and is streamed when requested by the user. That is, content 304 is played back as it arrives on disk 310. One method of achieving this functionality is by using a separate module such as DRM proxy 308 for retrieving the content from content server 302, using a receipt 306. It should be noted that DRM proxy 308 is separate and apart from content player 312 because frequent modifications to the module may be carried out as proves necessary, without modifying other components.

Alternatively, a module which functions as part of the content player 312 may carry out the streaming functionality. Examples of content players which are currently available on the market are Quicktime 4™ available from Apple Computer, Inc.®, RealPlayer™ available from RealNetworks, Inc.® and Shockwave 7™ available from MacroMedia, Inc.®. Further, in the on-line mode also referred to as "pay-to-view" mode, the license is delivered concurrently with content 304. Although not shown, it will be apparent to one of ordinary skill in the art that various permutations of modules and modes for retrieving encrypted content 304 are possible.

Fig. 4 is a schematic block diagram of zipLock system 400 for enabling playback of content files 404 according to the present invention. Advantageously, system 400 allows only authorized users to playback content files in accordance with one embodiment.

System 400 comprises content server 402, among other components, for downloading content files 404 to content player 408 for the purpose of allowing playback of the content files. During playback, content player 408 begins by retrieving a chunk of content from content files 404, each file including a content header (described in Fig. 2) for identifying a license name, a content identification, and a license server URL among other information. Thereafter, the chunk of content is handed over to player module 410, which begins to coordinate the decryption of content files 404. Player module 410 contacts DRM core 414 to request a session key for decrypting the content files. Because the requested key is contained within a license, DRM core 414 must identify the appropriate license and its current location. This is accomplished by reading the content header to identify the license name, the content identification, and a lieense server 406

wherever the license is located. In some instances, DRM core 414 checks to see whether the license is stored within license store 415 and retrieves the license if found. Otherwise, the identified license server URL is contacted to request a license.

In addition, license data generator 416 provides DRM core 414 with a machine identification which is unique to the end user's machine for comparison with the header information. Using all of the obtained information, DRM core 414 through DRM module 420 contacts license server 406 to request the session key and status data for the given machine. Advantageously, the session key is a single session key, meaning that it enables playback of the encrypted files only for a single session.

To obtain the session key, DRM module 420 responds by directing DRM proxy 422 to contact and obtain a license (which contains the session key) from license server 406. Upon successful verification of the license terms, license server 406 delivers the license that contains the session key. DRM proxy 422 passes the license back to DRM module 420, which in turn forwards it to DRM core 414. DRM core 414 retrieves the session key and passes the key securely back to player module 410. In turn, player module 410 forwards the key and encrypted content files 404 to DRM decoder 412 which executes the decryption process and returns the decrypted files to player module 410. Finally, content player 410 passes the decrypted content files content player 408 for playback.

It should be noted that the preceding steps are only performed for the first chunk of encrypted content after which subsequent chunks are automatically played back. Further, it should be observed that there are implications for the player module 410 when it hands encrypted content to the decoder module 412, because content is encrypted on a frame-by-frame basis. This makes seeking a specific location and the content a little more difficult and, as such, the decoder module may be provided with API (application programming interface) to aid the caller in dealing with these frames. In this manner, the present invention enables system 400 to upload encrypted content files 404 and play back those content files using a content player module 410.

Fig. 5 is a block diagram of zipLock system 500 for acquiring a license which authorizes user playback of a content file.

In Fig. 5, as shown in an exemplary embodiment, system 500 includes client and server sides 522 and 520. Among other components, client side 522 includes DRM proxy 504 for preparing data for a license request, module 506 for building a

license request message, DRM core 508 for obtaining machine specific information from license data generator 510, and license database 512 for storing license files.

In a typical operation, the user purchases content such as music recordings (for example) from the store front at a website (not shown). Numerous websites are available for purchasing various types of digital content including Disney.com®, Sony.com®, and Shockwave.com®, for example. Using a web browser or a program that is capable of posting a web form to server 516, the user initiates the transaction with the appropriate website. The transaction typically involves several round trips to the web site with the transaction concluding with a request for a box file 502. Box file 502 is a file that describes the content requested by the user, and in one embodiment has a .cBox extension.

DRM proxy 504 contains a box file handler and is registered with system 500 as the handler for files with the .cBox extension. When box file 502 is received, DRM proxy 504 directs module 506 to build a license request message for forwarding to license server 516. In one embodiment, this request is in XML (extensible markup language) format. Module 506 queries the machine identification to be included in the license request. Thereafter, DRM proxy 504 starts a network job which sends the license request message to license server 516. License server 516, in one embodiment is a CGI (common gateway interface) program available through license server 516.

Upon receipt of the license request, license server 516 verifies that the content file has been purchased prior to continuing with the processing of the license request. zipLock data base 514 contains the terms of the license along with the keys for decrypting the content file. These terms are retrieved and forwarded to license generator 518. It should be observed that a different license generator is implemented for each digital rights management solution being employed on client side 522. License generator 518 generates the license which includes the terms of the license. Also included within the license, are the keys for decrypting the content file.

It should be observed that the content decryption keys are bound to the particular machine located on the client side 522. By way of example, particular information that is unique to the machine such as the machine identification number is bound to the license. In this way, the present invention implements a machine-binding solution which allows digital content playback only on a particular machine. Upon receiving the license from license generator 518, license server 516 forwards the license over the network to DRM proxy 504. In turn, DRM proxy forwards the license to module

506 for DRM-specific processing. DRM core 508 retrieves the license and stores the license within database 512.

Although not shown, the process for retrieving a license may oecur subsequent to a purchase transaction such as when the user wishes to play back content offline. Further, license acquisition can also occur when there is no financial transaction involved; for example, when the user requests a trial license. A trial license permits a user to utilize the content files for a specific period after which the trial license expires. Table 1 below illustrates exemplary steps taken by system 500 to acquire a license when there is no financial transaction involved.

1.	A content player (not shown) asks DRM core 508 to play a content.
2.	DRM core 508 checks its local store, e.g., license store 512, and finds there is no valid license available (it finds no license or license is expired).
3.	DRM core 508 fields a license request message with the machine identification.
4.	DRM core 508 invokes DRM proxy 504 to send a license request message.
5.	DRM proxy starts a network job to send a license request message to license server 516.
6.	License server 516 presents a page to collect license terms desired by the user and supported by system 500 before continuing with the processing of license request.
7.	The terms of the license are collected and sent to data base 514.
8.	The license request, along with the terms of the license and keys for decryption, are retrieved from data base 514 and are dispatched to license generator 518.
9.	The license is generated from the obtained information.
10.	The license data is returned to server 516.
11.	License data is returned over the network to the DRM proxy 504.
12.	DRM proxy 504 passes the license response message to DRM 506 for DRM-specific processing.
13.	DRM module 506 via DRM core 508 saves the license data in its license store 512 in its own specific way.

Table 1

The present invention advantageously separates a portion of the content from the original content file until decryption time to prevent unauthorized content usage. Moreover, licenses are bound to particular machines so that copying the content to a machine other than the authorized machine is futile. The present invention also utilizes a secure data channel in which the content keys are passed in secured format. Code obfuscation is used to hide code that handles decrypted data.

Other advantages include the implementation of the DRM core and the DRM decoder within separate modules to increase the complexity for hackers, and the employment of session key-based on-line license verification to maximize security. In this manner, the system of the present invention manages rights to one or more digital content files within a computer network and limits the playback of such content files to an authorized user. Furthermore, the present invention facilitates distribution and content production, which ultimately results in a shorter product development cycle.

While the above is a complete description of exemplary specific embodiments of the invention, additional embodiments are also possible. Thus, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims along with their full scope of equivalents.

WHAT IS CLAIMED IS:

1. A system for encrypting a content file within a computer network for on-line playback, the system comprising:

a first key for decrypting the content file;

a header which contains information that allows playback of the content file;

a key module for generating the first key; and

a content module for encrypting the content file, and for removing a first content portion of the content file and substituting the header thereof.

2. The system of claim 1 further comprising

a license that contains both the first key and the first content portion.

3. The system of claim 1 wherein the information is any one of a name for a license, an identifier for the content file, and an URL (uniform resource locator) of a license server for generating the license.

4. The system of claim 1 wherein the content module segments the content file into first and second segments.

5. The system of claim 4 further comprising

a second key, wherein the content module encrypts the first and second segments of the content file using the first and second keys, respectively.

6. A method by a computer system, for encrypting a content file to permit on-line play back of the content file, the method comprising:

generating a first key for decrypting the content file;

creating a header which contains a first field that contains information for enabling playback of the content file;

removing a first portion of the content file and substituting the header thereof; and

encrypting the content file such that the content file is decrypt-able using the first key.

7. The method of claim 6 further comprising

including the first portion and the first key in a license for authorizing playback of the content file.

8. The method of claim 6 further comprising

receiving the license containing the first key and the first portion,

decrypting the content file using the first key, and

combining the first portion with the content file.

9. A system for managing rights to a content file within a computer network, and to permit an authorized user to playback the content file online, the system comprising:

a key for decrypting the content file;

a database for storing the key;

a license having the key for authorizing decryption and playback of the content file;

a license server system having at least one license server, the system generating the license for forwarding to the authorized user;

a first computer system for generating the content file, the first computer system further comprising,

a header which contains information relating to a name for the license, identification of the content file, and an URL (uniform resource locator) of the license server,

an encoder module for creating the header,

a key module for generating the key,

a content module for encrypting the content file using the key, and for removing a portion of the content file and substituting the header thereof;

a communication network for streaming the content file and transmitting the license to the authorized user;

a second computer system for receiving the content file and the license via the communication network, the second computer system further comprising,

a decoder module for decrypting the content file using the key, upon receipt of the license;

a license data generator for generating identification information about a computer wherein the content file is played back,

a core module for retrieving the identification information from the license data generator,

a license database for storing the license when received;

a content player which plays back the content file when unencrypted,

a proxy module for sending a request to obtain the license from the license server; and

a request module for forwarding the request to obtain the license to the proxy module.

10. The system of claim 9 wherein the license server system dynamically generates the license when requested by the authorized user while online.

11. A system for managing rights to a content file within a computer network, and to permit an authorized user to playback the content file online, the system comprising:

a key for decrypting the content file;

a first content portion which is part of the content file;

a license for decrypting the content file, the license containing both the key and the first content portion;

a license server system having at least one license server, the system generating the license for forwarding to the authorized user;

a first computer system for generating the content file, the first computer system further comprising,

a header which contains a first field for having identification information;

software containing one of more instructions for creating the header,

software containing one or more instructions for generating the key,

software containing one or more instructions for encrypting the content file, and for removing the first content portion from the content file and substituting the header thereof;

a communication network for transmitting the content file and the license; and

a second computer system for receiving the content file and the license via the communication network, the second computer system further comprising,

software containing one or more instructions for streaming the content file while the user is online, and to permit playback of the content file when unencrypted,

software containing one or more instructions for decrypting the content file using the key, upon receipt of the license, and

software containing one or more instructions for combining the first content portion with the content file.

12. In a computer network, a method using a license for enabling playback of a content file, the content file containing a header which identifies the license and the content file, the license including both a first portion of the content file and a session key that enables decryption of the content file, the method comprising:

streaming the content file to an authorized user system;

retrieving the license which contains the session key and the first portion of the content;

for a single playback session, decrypting the content file using the session key; and

combining the first portion with the content file during playback.

13. The method of claim 12 further comprising

dynamically generating the license prior to the step of retrieving the license.

14. The method of claim 12 further comprising

storing the license prior to the step of retrieving the license.

15. In a computer network, a method for obtaining a license from a license server to authorize on-line playback of a content file, the license containing a session key and a portion of the content file, the method comprising:

requesting the license from the license server;

providing the license server with information relating to the terms of the license and a machine identification wherein the content file is played back;

binding the license to a machine with the machine identification so that the content file is playable only on the machine so designated; and

forwarding the license having the session key and the portion of the content file to the machine.

16. The method of claim 15 further comprising

obtaining a box receipt file prior to the step of requesting the license from the license server.

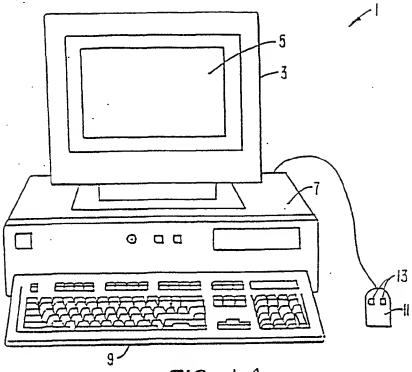

1
5
3
7
13
11
9

FIG. 1A

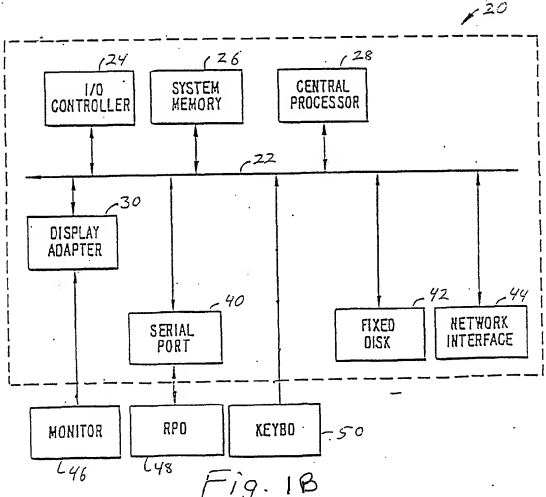

20
24
I/O CONTROLLER
26
SYSTEM MEMORY
28
CENTRAL PROCESSOR
22
30
DISPLAY ADAPTER
40
SERIAL PORT
42
FIXED DISK
44
NETWORK INTERFACE
MONITOR
RPO
KEYBO
50
46
48

Fig. 1B

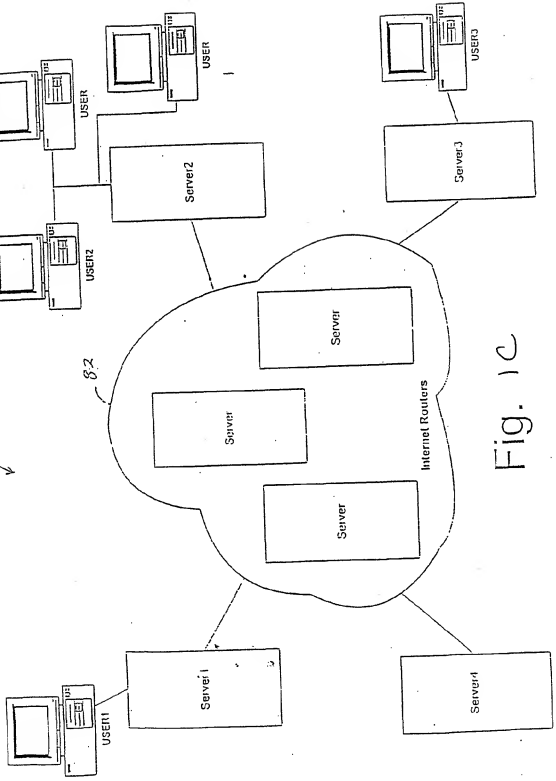

USER1
USER2
USER
USER
USER3
Server1
Server2
Server3
Server
Server
Server
Internet Routers
82
84
86

Fig. 1C

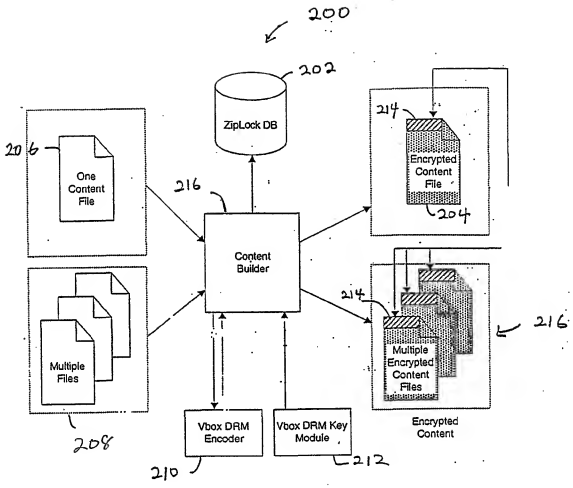

200
202
ZipLock DB
206
One Content File
216
Content Builder
214
Encrypted Content File
204
Multiple Files
208
214
Multiple Encrypted Content Files
216
Encrypted Content
Vbox DRM Encoder
210
Vbox DRM Key Module
212

Fig. 2

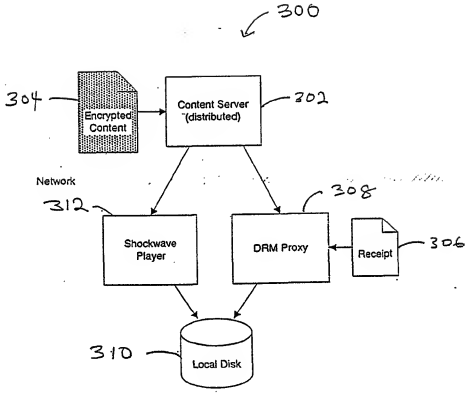

300
304
Encrypted Content
Content Server (distributed)
302
Network
312
308
Shockwave Player
DRM Proxy
Receipt
306
310
Local Disk

Fig. 3

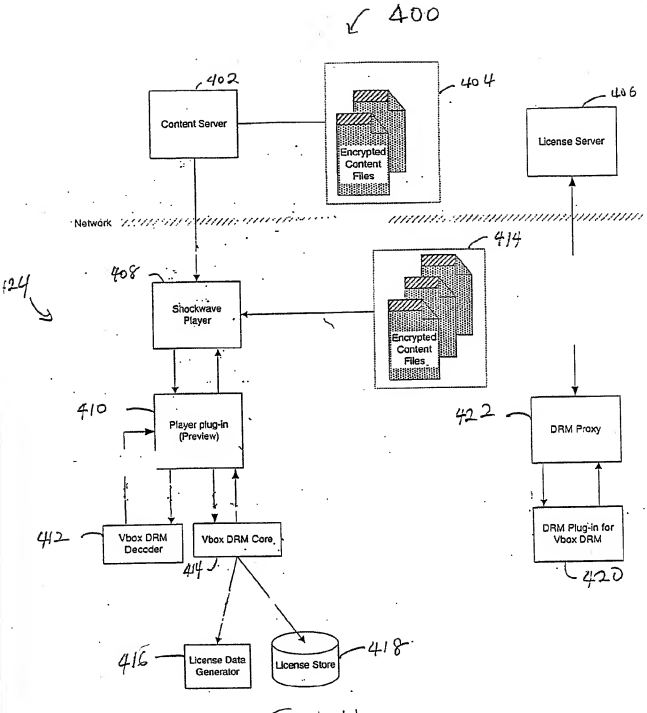

400
402
Content Server
404
Encrypted Content Files
406
License Server
Network
414
424
408
Shockwave Player
Encrypted Content Files
410
Player plug-in (Preview)
422
DRM Proxy
412
Vbox DRM Decoder
Vbox DRM Core
414
DRM Plug-in for Vbox DRM
420
416
License Data Generator
418
License Store

Fig. 4

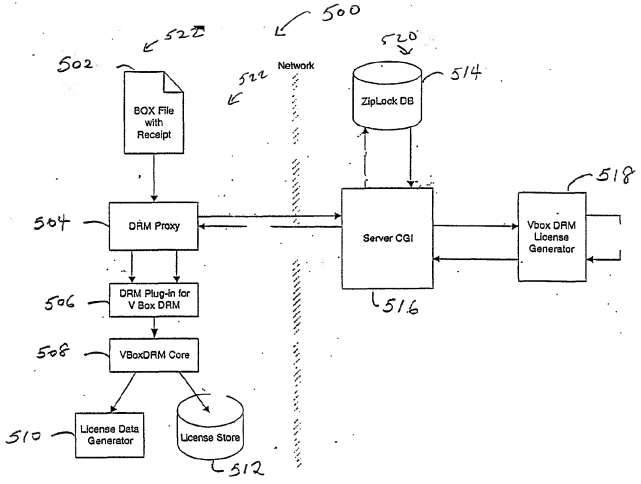

500
520
502
Network
522
514
BOX File with Receipt
ZipLock DB
518
504
DRM Proxy
Server CGI
Vbox DRM License Generator
506
DRM Plug-in for V Box DRM
516
508
VBoxDRM Core
510
License Data Generator
License Store
512

Fig. 5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/023315 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/26495

(22) International Filing Date: 24 August 2001 (24.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/659,902 12 September 2000 (12.09.2000) US

(71) Applicant: ALADDIN KNOWLEDGE SYSTEMS, LTD. [IL/IL]; 15, Beit Oved Street, Tel Aviv 61110 (IL).

(72) Inventors: XU, Biu; 955 La Mesa Terrace, Unit-I, Sunnyvale, CA 94086 (US). LI, Weijun; 687 Ontario Court, # 8, Sunnyvale, CA 94087 (US). SMITH, Kyle; 394 Vale Drive, San Jose, CA 95123 (US). BAO, Dalun; 200 E. Dana St. D85, Mountain View, CA 94041 (US).

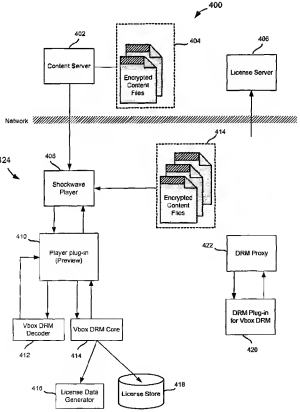
(74) Agents: NWAMU, Fidel, D. et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT



(57) Abstract: A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.

WO 02/023315 A3

WO 02/023315 A3

Published:
— *with international search report*

(88) Date of publication of the international search report:
7 August 2003

(15) Information about Correction:

Previous Correction:
see PCT Gazette No. 51/2002 of 19 December 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/26495

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 42098 A (CRYPTOWORKS INC) 24 September 1998 (1998-09-24) figure 1 abstract page 1, line 5 - line 6 page 1, line 11 - line 13 page 5, line 16 - line 18 page 5, line 20 - line 24 page 5, line 33 -page 6, line 2 page 6, line 6 - line 20 page 9, line 29 - line 30 page 10, line 11 - line 17 page 10, line 25 - line 32 page 11, line 3 - line 5 page 11, line 8 - line 15 page 14, line 22 - line 23 page 15, line 3 - line 4 page 15, line 7 - line 9 page 16, line 13 - line 15 -/--	1-15

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 January 2003	10/02/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Chabot, P

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 16, line 18 - line 28 page 16, line 31 -page 17, line 2 page 17, line 6 - line 9 page 17, line 13 - line 20 page 17, line 26 - line 27 page 18, line 19 - line 34 page 19, line 12 - line 14 page 19, line 19 - line 21 page 20, line 14 - line 20 page 21, line 3 - line 12 page 21, line 20 - line 23 page 25, line 16 - line 21 page 26, line 13 - line 15 page 26, line 32 -page 27, line 2 page 28, line 4 - line 7 page 28, line 9 - line 23	
A	US 5 754 646 A (WILLIAMS THOMAS H ET AL) 19 May 1998 (1998-05-19) column 2, line 51 -column 3, line 25 column 3, line 56 -column 4, line 29	1-8
A	US 5 222 134 A (WAITE DAVID P ET AL) 22 June 1993 (1993-06-22) column 2, line 54 - line 68 column 3, line 57 - line 62 column 4, line 58 - line 63 column 4, line 66 - line 68	1-8
A	NOGHANI B S ET AL: "REDUCING LATENCY ON THE INTERNET USING COMPONENT-BASED DOWNLOAD AND FILE-SEGMENT TRANSFER PROTOCOL: EXPERIMENTAL RESULTS" PROCEEDINGS OF THE SYMPOSIUM OF PERFORMANCE EVALUATION OF COMPUTER AND TELECOMMUNICATION SYSTEMS, XX, XX, 16 July 2000 (2000-07-16), pages 324-331, XP001012275 abstract	1-16
A	US 5 999 622 A (KUROSAWA TAKASHI ET AL) 7 December 1999 (1999-12-07) abstract	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/26495

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9842098	A	24-09-1998	AU	6759198 A	12-10-1998
			EP	0968585 A1	05-01-2000
			WO	9842098 A1	24-09-1998
US 5754646	A	19-05-1998	CA	2227060 A1	06-02-1997
			GB	2317476 A ,B	25-03-1998
			WO	9704412 A2	06-02-1997
US 5222134	A	22-06-1993	US	5103476 A	07-04-1992
			AT	171024 T	15-09-1998
			CA	2095723 A1	08-05-1992
			DE	69130175 D1	15-10-1998
			DE	69130175 T2	10-02-2000
			EP	0556305 A1	25-08-1993
			JP	7089345 B	27-09-1995
			JP	6501120 T	27-01-1994
			WO	9209160 A1	29-05-1992
US 5999622	A	07-12-1999	NONE		

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/023315 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/26495

(22) International Filing Date: 24 August 2001 (24.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/659,902 12 September 2000 (12.09.2000) US

(71) Applicant: ALADDIN KNOWLEDGE SYSTEMS, LTD. [IL/IL]; 15, Beit Oved Street, Tel Aviv 61110 (IL).

(72) Inventors: XU, Bin; 955 La Mesa Terrace, Unit-I, Sunnyvale, CA 94086 (US). LI, Weijun; 687 Ontario Court, # 8, Sunnyvale, CA 94087 (US). SMITH, Kyle; 394 Vale Drive, San Jose, CA 95123 (US). BAO, Dalun; 200 E. Dana St. D85, Mountain View, CA 94041 (US).

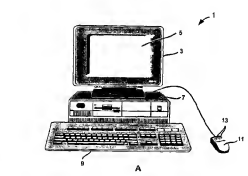
(74) Agents: NWAMU, Fidel, D. et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111 (US).

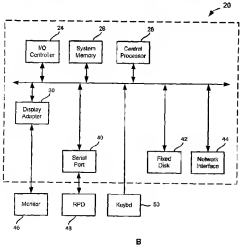
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT





(57) Abstract: A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.

WO 02/023315 A2

patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

(48) Date of publication of this corrected version:
19 December 2002

(15) Information about Correction:
see PCT Gazette No. 51/2002 of 19 December 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT

BACKGROUND OF THE INVENTION

This invention relates to the field of information processing and more particularly to systems for implementing digital management rights.

Millions of users currently have access to more information than at any period in the history of society. Specifically, digital content such as interactive web content, musical recordings, medical and financial forms, automatic banking, facsimiles, and various other forms of audio and video content are widely accessible.

Although attributable to a number of reasons, the widespread access to digital content has been a result of the development of electronic compuer networks, and Internet in particular. Another reason relates to the increase in available bandwidth and the availability of compression technology for transferring large amounts of content. In addition, numerous sites and bulletin boards post content for distribution to users. Content providers such as publishers of books and magazines, information database providers, and producers of music, video games, and images are distributing content in digital form over the Internet. In fact, some providers of interactive web content and music provide interactive web players for playing back content. Examples of such interactive web players which are currently available on the market are Quicktime 4™ available from Apple Computer, Inc.®, RealPlayer™ available from RealNetworks, Inc. ® and Shockwave 7™ available from MacroMedia, Inc. ®

While access to digital content has been widely beneficial, a fundamental problem facing content providers is how to prevent the unauthorized use and distribution of digital content. Content providers are concerned with getting compensated for their work. Unauthorized copying and use of content providers works deprives rightful owners of billions of dollars according to a well-known source. Unauthorized copying is exercebated because consumers can easily retrieve content, and technology is available for perfectly reproducing content.

A number of mechanisms have been developed to protect against unauthorized access and duplication and to provide digital rights management. One method is a digital rights management system that allows a set of rules to determine how the content is used. Another method (for software) for curbing unauthorized duplication

is the use of a scheme which provides software tryouts or demos that typically work and expire after a specific duration. Other methods use a copy protection scheme that limits the number of copies that a user can make, after which additional copying results in corrupt copies. Further, an alternate scheme requires the presence of a license on a client workstation for the software to operate.

Many of the aforementioned schemes are typically implemented using "encryption/decryption" of the digital content. Encryption is the conversion of data into an unintelligible form, e.g., ciphertext, that cannot be easily understood by unauthorized users. Decryption is the process of converting encrypted content back into its original form such that the it becomes intelligible. Simple ciphers include the rotation of letters in the alphabet, the substitution of letters for numbers, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital information content.

In order to easily recover the encrypted information content, the correct decryption key is required. The key is an algorithm that decodes the work of the encryption algorithm. The more complex the encryption algorithm, the more difficult it becomes to decode the communications without access to the key. Generally, there are two types of key schemes for encryption/decryption systems, namely (1) Public Key Systems (PKS) or asymmetric systems which utilize two different keys, one for encryption, or signing, and one for decryption, or verifying; and (2) nonpublic key systems that are known as symmetric, or secret key, systems.

Although the use of public or private key can be an effective way to prevent access to digital content, the transfer of keys often requires extensive coordination with the end user. Also, the use of keys in the related art does not always provide flexible licensing arrangements, or an efficient way to handle many instances of different deliverable digital content products.

Therefore, there is a need to resolve the aforementioned problem relating to conventional approaches for protecting digital information particularly with regard to managing the digital rights for on-line distribution of interactive web content and music.

SUMMARY OF THE INVENTION

A system for managing rights to a content file within a computer network. The system permits streaming and allows an authorized user to play back the content file

while the user is online. In one embodiment, the system comprises a key for decrypting the content file, a license which contains the key for authorizing decryption and playback of the content file and a header which contains information relating to a name for the license, identification of the content file, and a URL (uniform resource locator) of the server. Advantageously, a content module encrypts the content file, removes a portion of the content file and substitutes the header thereof.

Upon request, a user's computer system receives the content file and the license via a communication network. When the content file and the license have been received, a decoder module decrypts the content file using the key, which is contained within the license. In a further aspect, a license data generator generates a machine identification to which the license is bound so that the content file is playable only on the designated machine. The system further includes a core module for retrieving the identification information from the license data generator, a license database for storing the license when received, and a content player which plays back the content file when it is unencrypted. In this manner, the present invention permits both playback of the content file and management of the corresponding rights to the content file without the disadvantages associated with the related art.

In one embodiment, the present invention provides a system for encrypting a content file within a computer network for on-line playback. The system comprises a first key for decrypting the content file and a header which contains information that allows playback of the content file. Other components include a key module for generating the first key, and a content module for encrypting the content file, and for removing a first content portion of the content file and substituting the header thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is an illustration of computer system 1 including display 3 having display screen 5.

Fig. 1B illustrates subsystems that might typically be found in a computer such as computer 1.

Fig. 1C is a generalized diagram of a typical network.

Fig. 2 is a block diagram of a zipLock system for encrypting content files according to the present invention.

Fig. 3 is a schematic block diagram of a zipLock delivery system for delivering encrypted content to an end user disk.

Fig. 4 is a schematic block diagram of a zipLock system for enabling playback of content files according to the present invention.

Fig. 5 is a block diagram of a zipLock system for acquiring a license which authorizes a user to playback a content file.

DETAILED DESCRIPTION OF THE DIAGRAMS

Overview

A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.

Therefore, at the very least, one or more keys and a license are required in order for a user to play back a content file. In this manner, the present system manages digital rights pertaining to such content files in accordance with one embodiment of the present invention. The present invention will be further understood with reference to the diagrams and descriptions which follow.

Description of Hardware

Fig. 1A is an illustration of computer system 1 including display 3 having display screen 5. Cabinet 7 houses standard computer components (not shown) such as a disk drive, CDROM drive, display adapter, network card, random access memory (RAM), central processing unit (CPU), and other components, subsystems and devices. User input devices such as mouse 11 having buttons 13, and keyboard 9 are shown. Other user input devices such as a trackball, touch-screen, digitizing tablet, etc. can be used. In general, the computer system is illustrative of but one type of computer system, such as a desktop computer, suitable for use with the present invention. Computers can be

configured with many different hardware components and can be made in many dimensions and styles (e.g., laptop, palmtop, pen top, server, workstation, mainframe). Any hardware platform suitable for performing the processing described herein is suitable for use with the present invention.

Fig. 1B illustrates subsystems that might typically be found in a computer such as computer 1.

In Fig. 1B, subsystems within box 20 are directly interfaced to internal bus 22. Such subsystems typically are contained within the computer system such as within cabinet 7 of Fig. 1A. Subsystems include input/output (I/O) controller 24, System Random Access Memory (RAM) 26, Central Processing Unit (CPU) 28, Display Adapter 30, Serial Port 40, Fixed Disk 42 and Network Interface Adapter 44. The use of bus 22 allows each of the subsystems to transfer data among the subsystems and, most importantly, with the CPU. External devices can communicate with the CPU or other subsystems via bus 22 by interfacing with a subsystem on the bus. Monitor 46 connects to the bus through Display Adapter 30. A relative pointing device (RPD) 48 such as a mouse connects through Serial Port 40. Some devices such as Keyboard 50 can communicate with the CPU by direct means without using the main data bus as, for example, via an interrupt controller and associated registers (not shown).

As with the external physical configuration shown in Fig. 1A, many subsystem configurations are possible. Fig. 1B is illustrative of but one suitable configuration. Subsystems, components or devices other than those shown in Fig. 1B can be added. A suitable computer system can be achieved without using all of the subsystems shown in Fig. 1. For example, a standalone computer need not be coupled to a network so Network Interface 44 would not be required. Other subsystems such as a CDROM drive, graphics accelerator, etc. can be included in the configuration without affecting the performance of the system of the present invention.

Fig. 1C is a generalized diagram of a typical network.

In Fig. 1C, the network system 80 includes several local networks coupled to the Internet. Although specific network protocols, physical layers, topologies, and other network properties are presented herein, the present invention is suitable for use with any network.

In Fig. 1C, computer USER1 is connected to Server1. This connection can be by a network such as Ethernet, Asynchronous Transfer Mode, IEEE standard 1553 bus, modem connection, Universal Serial Bus, etc. The communication link need not be a

wire but can be infrared, radio wave transmission, etc. Server1 is coupled to the Internet. The Internet is shown symbolically as a collection of server routers 82. Note that the use of the Internet for distribution or communication of information is not strictly necessary to practice the present invention but is merely used to illustrate a preferred embodiment, below. Further, the use of server computers and the designation of server and client machines is not crucial to an implementation of the present invention. USER1 Computer can be connected directly to the Internet. Server1's connection to the Internet is typically by a relatively high bandwidth transmission medium such as a T1 or T3 line.

Similarly, other computers at 84 are shown utilizing a local network at a different location from USER1 computer. The computers at 84 are coupled to the Internet via Server2. USER3 and Server3 represent yet a third installation.

Note that the concepts of "client" and "server," as used in this application and the industry, are very loosely defined and, in fact, are not fixed with respect to machines or software processes executing on the machines. Typically, a server is a machine or process that is providing information to another machine or process, i.e., the "client," that requests the information. In this respect, a computer or process can be acting as a client at one point in time (because it is requesting information) and can be acting as a server at another point in time (because it is providing information). Some computers are consistently referred to as "servers" because they usually act as a repository for a large amount of information that is often requested. For example, a World Wide Web (WWW, or simply, "Web") site is often hosted by a server computer with a large storage capacity, high-speed processor and Internet link having the ability to handle many high-bandwidth communication lines.

A server machine will most likely not be manually operated by a human user on a continual basis, but, instead, has software for constantly, and automatically, responding to information requests. On the other hand, some machines, such as desktop computers, are typically thought of as client machines because they are primarily used to obtain information from the Internet for a user operating the machine.

Depending on the specific software executing at any point in time on these machines, the machine may actually be performing the role of a client or server, as the need may be. For example, a user's desktop computer can provide information to another desktop computer. Or a server may directly communicate with another server computer. Sometimes this is characterized as "peer-to-peer," communication. Although processes of the present invention, and the hardware executing the processes, may be characterized

by language common to a discussion of the Internet (e.g., "client," "server," "peer") it should be apparent that software of the present invention can execute on any type of suitable hardware including networks other than the Internet.

Although software of the present invention, may be presented as a single entity, such software is readily able to be executed on multiple machines. That is, there may be multiple instances of a given software program, a single program may be executing on two or more processors in a distributed processing environment, parts of a single program may be executing on different physical machines, etc. Further, two different programs, such as a client and server program, can be executing in a single machine, or in different machines. A single program can be operating as a client for one information transaction and as a server for a different information transaction.

Details of Embodiments of the Present Invention

A first embodiment of the present invention is incorporated into a product called "zipLock"™ available from a primary company Preview Systems, Inc.® of Sunnyvale, California.

Fig. 2 is a block diagram of zipLock system 200 for encrypting content files according to the present invention. As used herein, the term "content" refers to digital information.

In Fig. 2, among other components, system 200 comprises content builder module 216 for encrypting one or more digital files, DRM encoder 210 for coordinating encryption as well as providing a header, DRM key module 212 for associating the information contained within a content file with a license, and zipLock database 202 for storing key sheaves received from content builder 212.

In a typical content encryption procedure, content builder 216 receives a single unencrypted content file 206 (or multiple unencrypted content files 208) for encryption. Content files 206 may be a musical recording, an audio or video image, which may be from third party sources or directly from the content providers. Upon receiving content file 206, content builder 216 utilizes an encryption algorithm to implement the encryption process. In one embodiment, this process is accomplished by segmenting content file 206 into variable segments, each segment being encrypted with a separate key.

A "key" may be a variable value that is applied to content file 206 using an algorithm to produce encryption text. A single key or multiple keys having constant or

variable lengths may be employed depending on which embodiment is implemented. After the encryption process, the keys are saved in zipLock database 202 for later retrieval during the playback process. In an exemplary embodiment, database 202 is an industry standard database system such as Oracle 8™ available from Oracle, Inc.®

Content builder 216 also functions to interact with database 202 to create the necessary information to enable the sale, distribution and tracking of the content within system 200. Advantageously, during the encryption process, content builder 216 removes a portion of content file 206 and in its place inserts a header (not shown), supplied by DRM encoder 210. The removed portion is thereafter added to a license file for authorizing playback of the content file 206. Therefore, the removed portion is considered part of the keys. Depending on the embodiment being implemented, the removed portion may be added to a pre-configured license, the terms of which are predefined. During the playback process, the pre-configured license is then retrieved when its terms are the same as the user's transaction. Alternatively, the removed portion may be saved and later added to a license which is generated on the fly during the playback process. In any event, once the license is obtained, the removed portion is thereafter recombined with the original content portion during the playback process.

Advantageously, removing a portion of content file 206 also provides a measure of extra security as the removed portion of content file 206 remains unavailable until decryption time. Therefore, copying encrypted content to another machine is completely useless without the back binding license. A further reason for removing a portion of content file 206 to accommodate the header is to keep the content file the same length as the original file. In this manner, the process of seeking a specific location in content file 206 during the decryption process is simplified.

The header within content file 206 contains information fields such as the license name, the content file identification, and the license server URL (uniform resource locator). The license name field enables content file 206 to be associated with the license file (containing the removed content portion). The content identification field identifies the content file 206 while the license server URL points to the address of the license server where the license is generated (or located). Although a multiple-field header is not shown, one of ordinary skill in the art will realize that the header may contain multiple fields for identifying various types of information other than those referenced above.

Fig. 3 is a schematic block diagram of zipLock delivery system 300 for delivering encrypted content 304 to an end user disk 310.

In Fig. 3, delivery system 300 includes content server 302 for generating encrypted content 304, interactive web player 312 and DRM proxy 308 which provides an alternate means for retrieving encrypted content 304 from server 302. Although operable in a number of modes, in one embodiment, system 300 functions in an on-line mode. In this mode, content 304 remains on content server 302 and is streamed when requested by the user. That is, content 304 is played back as it arrives on disk 310. One method of achieving this functionality is by using a separate module such as DRM proxy 308 for retrieving the content from content server 302, using a receipt 306. It should be noted that DRM proxy 308 is separate and apart from content player 312 because frequent modifications to the module may be carried out as proves necessary, without modifying other components.

Alternatively, a module which functions as part of the content player 312 may carry out the streaming functionality. Examples of content players which are currently available on the market are Quicktime 4™ available from Apple Computer, Inc.®, RealPlayer™ available from RealNetworks, Inc.® and Shockwave 7™ available from MacroMedia, Inc.®. Further, in the on-line mode also referred to as "pay-to-view" mode, the license is delivered concurrently with content 304. Although not shown, it will be apparent to one of ordinary skill in the art that various permutations of modules and modes for retrieving encrypted content 304 are possible.

Fig. 4 is a schematic block diagram of zipLock system 400 for enabling playback of content files 404 according to the present invention. Advantageously, system 400 allows only authorized users to playback content files in accordance with one embodiment.

System 400 comprises content server 402, among other components, for downloading content files 404 to content player 408 for the purpose of allowing playback of the content files. During playback, content player 408 begins by retrieving a chunk of content from content files 404, each file including a content header (described in Fig. 2) for identifying a license name, a content identification, and a license server URL among other information. Thereafter, the chunk of content is handed over to player module 410, which begins to coordinate the decryption of content files 404. Player module 410 contacts DRM core 414 to request a session key for decrypting the content files. Because the requested key is contained within a license, DRM core 414 must identify the appropriate license and its current location. This is accomplished by reading the content header to identify the license name, the content identification, and a license server 406

wherever the license is located. In some instances, DRM core 414 checks to see whether the license is stored within license store 415 and retrieves the license if found. Otherwise, the identified license server URL is contacted to request a license.

In addition, license data generator 416 provides DRM core 414 with a machine identification which is unique to the end user's machine for comparison with the header information. Using all of the obtained information, DRM core 414 through DRM module 420 contacts license server 406 to request the session key and status data for the given machine. Advantageously, the session key is a single session key, meaning that it enables playback of the encrypted files only for a single session.

To obtain the session key, DRM module 420 responds by directing DRM proxy 422 to contact and obtain a license (which contains the session key) from license server 406. Upon successful verification of the license terms, license server 406 delivers the license that contains the session key. DRM proxy 422 passes the license back to DRM module 420, which in turn forwards it to DRM core 414. DRM core 414 retrieves the session key and passes the key securely back to player module 410. In turn, player module 410 forwards the key and encrypted content files 404 to DRM decoder 412 which executes the decryption process and returns the decrypted files to player module 410. Finally, content player 410 passes the decrypted content files content player 408 for playback.

It should be noted that the preceding steps are only performed for the first chunk of encrypted content after which subsequent chunks are automatically played back. Further, it should be observed that there are implications for the player module 410 when it hands encrypted content to the decoder module 412, because content is encrypted on a frame-by-frame basis. This makes seeking a specific location and the content a little more difficult and, as such, the decoder module may be provided with API (application programming interface) to aid the caller in dealing with these frames. In this manner, the present invention enables system 400 to upload encrypted content files 404 and play back those content files using a content player module 410.

Fig. 5 is a block diagram of zipLock system 500 for acquiring a license which authorizes user playback of a content file.

In Fig. 5, as shown in an exemplary embodiment, system 500 includes client and server sides 522 and 520. Among other components, client side 522 includes DRM proxy 504 for preparing data for a license request, module 506 for building a

license request message, DRM core 508 for obtaining machine specific information from license data generator 510, and license database 512 for storing license files.

In a typical operation, the user purchases content such as music recordings (for example) from the store front at a website (not shown). Numerous websites are available for purchasing various types of digital content including Disney.com®, Sony.com®, and Shockwave.com®, for example. Using a web browser or a program that is capable of posting a web form to server 516, the user initiates the transaction with the appropriate website. The transaction typically involves several round trips to the web site with the transaction concluding with a request for a box file 502. Box file 502 is a file that describes the content requested by the user, and in one embodiment has a .cBox extension.

DRM proxy 504 contains a box file handler and is registered with system 500 as the handler for files with the .cBox extension. When box file 502 is received, DRM proxy 504 directs module 506 to build a license request message for forwarding to license server 516. In one embodiment, this request is in XML (extensible markup language) format. Module 506 queries the machine identification to be included in the license request. Thereafter, DRM proxy 504 starts a network job which sends the license request message to license server 516. License server 516, in one embodiment is a CGI (common gateway interface) program available through license server 516.

Upon receipt of the license request, license server 516 verifies that the content file has been purchased prior to continuing with the processing of the license request. zipLock data base 514 contains the terms of the license along with the keys for decrypting the content file. These terms are retrieved and forwarded to license generator 518. It should be observed that a different license generator is implemented for each digital rights management solution being employed on client side 522. License generator 518 generates the license which includes the terms of the license. Also included within the license, are the keys for decrypting the content file.

It should be observed that the content decryption keys are bound to the particular machine located on the client side 522. By way of example, particular information that is unique to the machine such as the machine identification number is bound to the license. In this way, the present invention implements a machine-binding solution which allows digital content playback only on a particular machine. Upon receiving the license from license generator 518, license server 516 forwards the license over the network to DRM proxy 504. In turn, DRM proxy forwards the license to module

506 for DRM-specific processing. DRM core 508 retrieves the license and stores the license within database 512.

Although not shown, the process for retrieving a license may occur subsequent to a purchase transaction such as when the user wishes to play back content offline. Further, license acquisition can also occur when there is no financial transaction involved; for example, when the user requests a trial license. A trial license permits a user to utilize the content files for a specific period after which the trial license expires. Table 1 below illustrates exemplary steps taken by system 500 to acquire a license when there is no financial transaction involved.

1.	A content player (not shown) asks DRM core 508 to play a content.
2.	DRM core 508 checks its local store, e.g., license store 512, and finds there is no valid license available (it finds no license or license is expired).
3.	DRM core 508 fields a license request message with the machine identification.
4.	DRM core 508 invokes DRM proxy 504 to send a license request message.
5.	DRM proxy starts a network job to send a license request message to license server 516.
6.	License server 516 presents a page to collect license terms desired by the user and supported by system 500 before continuing with the processing of license request.
7.	The terms of the license are collected and sent to data base 514.
8.	The license request, along with the terms of the license and keys for decryption, are retrieved from data base 514 and are dispatched to license generator 518.
9.	The license is generated from the obtained information.
10.	The license data is returned to server 516.
11.	License data is returned over the network to the DRM proxy 504.
12.	DRM proxy 504 passes the license response message to DRM 506 for DRM-specific processing.
13.	DRM module 506 via DRM core 508 saves the license data in its license store 512 in its own specific way.

Table 1

The present invention advantageously separates a portion of the content from the original content file until decryption time to prevent unauthorized content usage. Moreover, licenses are bound to particular machines so that copying the content to a machine other than the authorized machine is futile. The present invention also utilizes a secure data channel in which the content keys are passed in secured format. Code obfuscation is used to hide code that handles decrypted data.

Other advantages include the implementation of the DRM core and the DRM decoder within separate modules to increase the complexity for hackers, and the employment of session key-based on-line license verification to maximize security. In this manner, the system of the present invention manages rights to one or more digital content files within a computer network and limits the playback of such content files to an authorized user. Furthermore, the present invention facilitates distribution and content production, which ultimately results in a shorter product development cycle.

While the above is a complete description of exemplary specific embodiments of the invention, additional embodiments are also possible. Thus, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims along with their full scope of equivalents.

WHAT IS CLAIMED IS:

1. A system for encrypting a content file within a computer network for on-line playback, the system comprising:

a first key for decrypting the content file;

a header which contains information that allows playback of the content file;

a key module for generating the first key; and

a content module for encrypting the content file, and for removing a first content portion of the content file and substituting the header thereof.

2. The system of claim 1 further comprising

a license that contains both the first key and the first content portion.

3. The system of claim 1 wherein the information is any one of a name for a license, an identifier for the content file, and an URL (uniform resource locator) of a license server for generating the license.

4. The system of claim 1 wherein the content module segments the content file into first and second segments.

5. The system of claim 4 further comprising

a second key, wherein the content module encrypts the first and second segments of the content file using the first and second keys, respectively.

6. A method by a computer system, for encrypting a content file to permit on-line play back of the content file, the method comprising:

generating a first key for decrypting the content file;

creating a header which contains a first field that contains information for enabling playback of the content file;

removing a first portion of the content file and substituting the header thereof; and

encrypting the content file such that the content file is decrypt-able using the first key.

7. The method of claim 6 further comprising

including the first portion and the first key in a license for authorizing playback of the content file.

8. The method of claim 6 further comprising

receiving the license containing the first key and the first portion,

decrypting the content file using the first key, and

combining the first portion with the content file.

9. A system for managing rights to a content file within a computer network, and to permit an authorized user to playback the content file online, the system comprising:

a key for decrypting the content file;

a database for storing the key;

a license having the key for authorizing decryption and playback of the content file;

a license server system having at least one license server, the system generating the license for forwarding to the authorized user;

a first computer system for generating the content file, the first computer system further comprising,

a header which contains information relating to a name for the license, identification of the content file, and an URL (uniform resource locator) of the license server,

an encoder module for creating the header,

a key module for generating the key,

a content module for encrypting the content file using the key, and for removing a portion of the content file and substituting the header thereof;

a communication network for streaming the content file and transmitting the license to the authorized user;

a second computer system for receiving the content file and the license via the communication network, the second computer system further comprising,

a decoder module for decrypting the content file using the key, upon receipt of the license;

a license data generator for generating identification information about a computer wherein the content file is played back,

a core module for retrieving the identification information from the license data generator,

a license database for storing the license when received;

a content player which plays back the content file when unencrypted,

a proxy module for sending a request to obtain the license from the license server; and

a request module for forwarding the request to obtain the license to the proxy module.

10. The system of claim 9 wherein the license server system dynamically generates the license when requested by the authorized user while online.

11. A system for managing rights to a content file within a computer network, and to permit an authorized user to playback the content file online, the system comprising:

a key for decrypting the content file;

a first content portion which is part of the content file;

a license for decrypting the content file, the license containing both the key and the first content portion;

a license server system having at least one license server, the system generating the license for forwarding to the authorized user;

a first computer system for generating the content file, the first computer system further comprising,

a header which contains a first field for having identification information;

software containing one of more instructions for creating the header,

software containing one or more instructions for generating the key,

software containing one or more instructions for encrypting the content file, and for removing the first content portion from the content file and substituting the header thereof;

a communication network for transmitting the content file and the license; and

a second computer system for receiving the content file and the license via the communication network, the second computer system further comprising,

software containing one or more instructions for streaming the content file while the user is online, and to permit playback of the content file when unencrypted,

software containing one or more instructions for decrypting the content file using the key, upon receipt of the license, and

software containing one or more instructions for combining the first content portion with the content file.

12. In a computer network, a method using a license for enabling playback of a content file, the content file containing a header which identifies the license and the content file, the license including both a first portion of the content file and a session key that enables decryption of the content file, the method comprising:

streaming the content file to an authorized user system;

retrieving the license which contains the session key and the first portion of the content;

for a single playback session, decrypting the content file using the session key; and

combining the first portion with the content file during playback.

13. The method of claim 12 further comprising

dynamically generating the license prior to the step of retrieving the license.

14. The method of claim 12 further comprising

storing the license prior to the step of retrieving the license.

15. In a computer network, a method for obtaining a license from a license server to authorize on-line playback of a content file, the license containing a session key and a portion of the content file, the method comprising:

requesting the license from the license server;

providing the license server with information relating to the terms of the license and a machine identification wherein the content file is played back;

binding the license to a machine with the machine identification so that the content file is playable only on the machine so designated; and

forwarding the license having the session key and the portion of the content file to the machine.

16. The method of claim 15 further comprising

obtaining a box receipt file prior to the step of requesting the license from the license server.

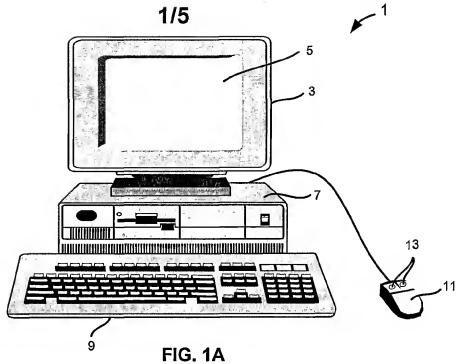

1
5
3
7
13
11
9

FIG. 1A

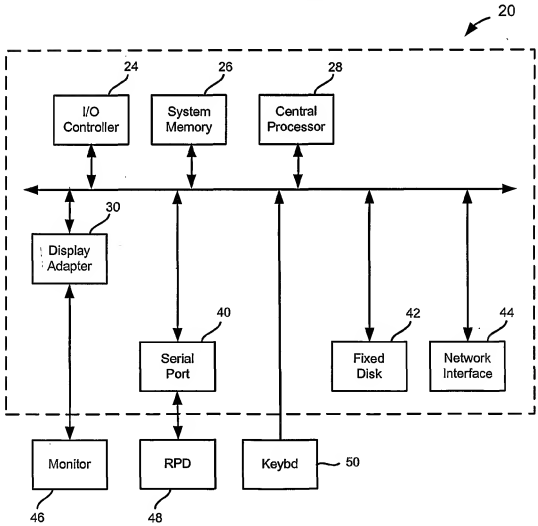

20
24
I/O Controller
26
System Memory
28
Central Processor
30
Display Adapter
40
Serial Port
42
Fixed Disk
44
Network Interface
Monitor
RPD
Keybd
50
46
48

FIG. 1B

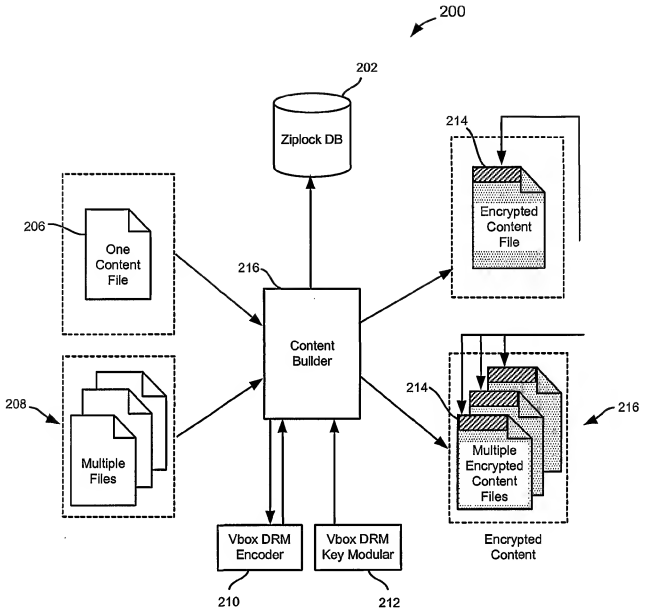

200
202
Ziplock DB
214
Encrypted Content File
206
One Content File
216
Content Builder
208
Multiple Files
214
216
Multiple Encrypted Content Files
Encrypted Content
Vbox DRM Encoder
Vbox DRM Key Modular
210
212

FIG. 2

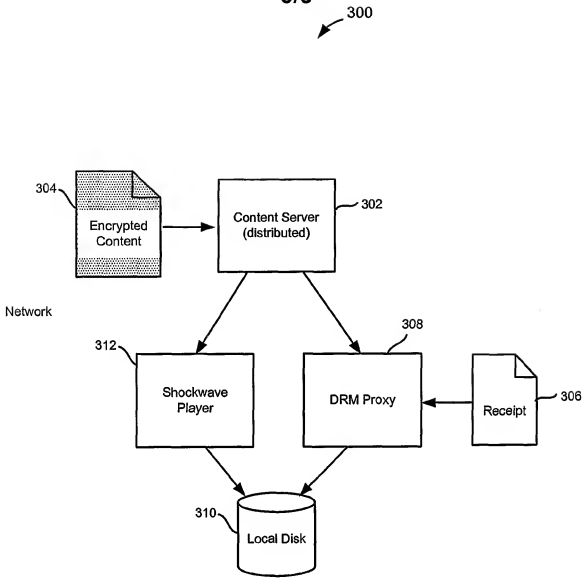

300
304
Encrypted Content
Content Server (distributed)
302
Network
312
Shockwave Player
308
DRM Proxy
Receipt
306
310
Local Disk

FIG. 3

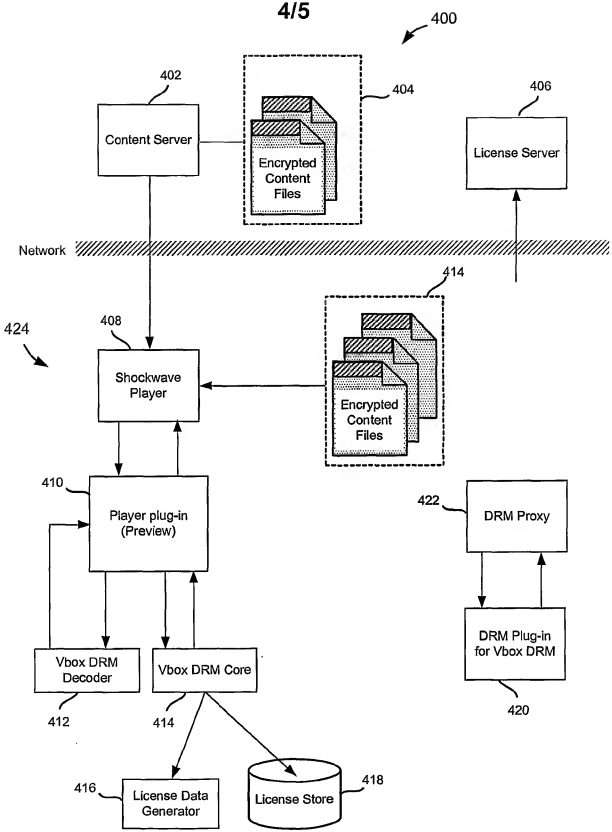

400
402
Content Server
404
Encrypted Content Files
406
License Server
Network
414
424
408
Shockwave Player
Encrypted Content Files
410
Player plug-in (Preview)
422
DRM Proxy
DRM Plug-in for Vbox DRM
420
Vbox DRM Decoder
412
Vbox DRM Core
414
416
License Data Generator
418
License Store

FIG. 4

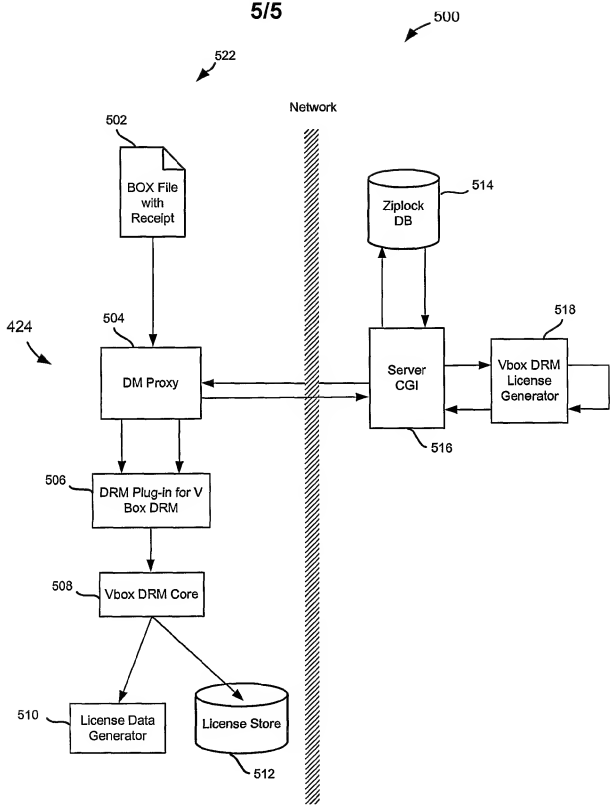

500
522
Network
502
BOX File with Receipt
514
Ziplock DB
518
424
504
DM Proxy
Server CGI
Vbox DRM License Generator
516
506
DRM Plug-In for V Box DRM
508
Vbox DRM Core
510
License Data Generator
License Store
512

FIG. 5